

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA  
ALEXANDRIA DIVISION**

HANAN ELATR KHASHOGGI,

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LTD.  
and Q CYBER TECHNOLOGIES LTD.,

Defendants.

Case No. 1:23-cv-779-LMB-LRVVAED

Action Filed: June 15, 2023

**NOTICE OF MOTION AND MOTION OF DEFENDANTS TO DISMISS COMPLAINT;  
MEMORANDUM OF POINTS AND AUTHORITIES**

TO THE COURT AND ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that Defendants NSO Group Technologies LTD. (“NSO”) and Q Cyber Technologies LTD. (“Q Cyber” and, collectively, “NSO”) will move the Court, the Honorable Leonie M. Brinkema, United States District Judge, for an order dismissing Plaintiff’s Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(2), and 12(b)(6), and the common law doctrine of *forum non conveniens*. This motion is based on this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the Declarations of Yaron Shohat (“Shohat Decl.”), Roy Blecher (“Blecher Decl.”), and Joseph N. Akrotirianakis (“Akro. Decl.”) submitted herewith, the pleadings, papers and records on file in this case, and such oral argument as may be presented at any hearing on this motion.

Counsel for Defendants is available for a hearing on this motion on October 27, 2023, but have been informed that Counsel for Plaintiff is not available on that day. Counsel for Defendants is not available for hearing on November 3, 2023, because Defendants are required to be present in the U.S. District Court for the Northern District of California for a hearing in another matter involving NSO. The Court will be closed on November 10, 2023, in honor of Veterans Day. Accordingly, Defendants respectfully request that the Court schedule a hearing on this motion for a date and time that is convenient to the Court.

DATED: September 29, 2023

KING & SPALDING LLP

By: /s/ Edmund Power

ASHLEY C. PARRISH (Bar No. 43089)

aparrish@kslaw.com

EDMUND POWER (Bar No. 65841)

epower@kslaw.com

KING & SPALDING LLP

1700 Washington Ave., NW, Suite 900

Washington, DC 20006

Telephone: (202) 737-0500

Facsimile: (202) 626-3737

JOSEPH N. AKROTIRIANAKIS (pro hac vice)

jakro@kslaw.com

KING & SPALDING LLP

633 West Fifth Street, Suite 1700

Los Angeles, CA 90071

Telephone: (213) 443-4355

Facsimile: (213) 443-4310

*Attorneys for Defendants NSO GROUP TECHS.  
LTD. and Q CYBER TECHS. LTD.*

## **TABLE OF CONTENTS**

INTRODUCTION .....	1
BACKGROUND .....	1
A. NSO’s technology and its use in preventing terrorism and other crimes. ....	1
B. Export control regulation of NSO’s operations. ....	3
C. Plaintiff and her allegations. ....	5
ARGUMENT .....	6
I. The Court Should Dismiss Because It Lacks Authority to Adjudicate This Case.....	6
A. The Court lacks subject-matter jurisdiction because NSO is entitled to derivative foreign sovereign immunity. ....	6
B. The Court lacks personal jurisdiction over NSO. ....	8
C. The act of state doctrine bars Plaintiff’s claims. ....	14
II. The Complaint Should Be Dismissed for <i>Forum Non Conveniens</i> .....	16
A. Israel is an adequate alternative forum.....	16
B. The “private factors” favor dismissal.....	17
C. The “public factors” also favor dismissal. ....	21
III. Plaintiff Does Not State a Claim Against NSO.....	22
A. Plaintiff does not state a CFAA claim.....	22
B. Plaintiff’s state law claims fail. ....	26
CONCLUSION.....	30

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>A Soc'y Without a Name v. Virginia</i> , 655 F.3d 342 (4th Cir. 2011) .....	25
<i>Advanced Fluid Sys. v. Huber</i> , 28 F. Supp. 3d 306 (M.D. Pa. 2014).....	26
<i>AdvanFort Co. v. Cartner</i> , 2015 WL 12516240 (E.D. Va. Oct. 30, 2015).....	14, 15
<i>Adventure Commc'ns, Inc. v. Ky. Registry of Election Fin.</i> , 191 F.3d 429 (4th Cir. 1999) .....	27
<i>Alhathloul v. DarkMatter Grp.</i> , 2023 WL 2537761 (D. Or. Mar. 16, 2023).....	13
<i>Alicog v. Kingdom of Saudi Arabia</i> , 860 F. Supp. 379 (S.D. Tex. 1994) .....	7
<i>Alicog v. Kingdom of Saudi Arabia</i> , 79 F.3d 1145 (5th Cir. 1996) .....	7
<i>Alternate Health USA Inc. v. Edalat</i> , 2022 WL 767573 (C.D. Cal. Mar. 14, 2022).....	20, 22
<i>Amoco Egypt Oil Co. v. Leonis Nav. Co.</i> , 1 F.3d 848 (9th Cir. 1993) .....	13
<i>Argoquest v. Israel Discount Bank, Ltd.</i> , 228 F. App'x 733 (9th Cir. 2007) .....	16
<i>Asahi Metal Indus. Co. v. Super. Ct.</i> , 480 U.S. 102 (1987).....	13
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	9
<i>Aziz v. Alcolac, Inc.</i> , 658 F.3d 388 (4th Cir. 2011) .....	26
<i>Blades of Green, Inc. v. Go Green Lawn &amp; Pest, LLC</i> , 2023 WL 5278654 (D. Md. Aug. 16, 2023) .....	24

<i>Broidy Cap. Mgmt., LLC v. Qatar,</i> 982 F.3d 582 (9th Cir. 2020) .....	8, 15
<i>Burns v. Gagnon,</i> 283 Va. 657 (2012) .....	29
<i>Butters v. Vance Int'l, Inc.,</i> 225 F.3d 462 (4th Cir. 2000) .....	7, 8
<i>Calendar Research LLC v. StubHub, Inc.,</i> 2020 WL 4390391 (C.D. Cal. May 13, 2020) .....	22
<i>Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.,</i> 334 F.3d 390 (4th Cir. 2003) .....	9
<i>Carolina Trucks &amp; Equip., Inc. v. Volvo Trucks of N. Am., Inc.,</i> 492 F.3d 484 (4th Cir. 2007) .....	27
<i>Casco Marine Paints &amp; Coatings, Ltd. v. M/V LEON,</i> 1996 WL 544232 (D. Md. June 20, 1996).....	19
<i>Cengiz v. Salman,</i> 2022 WL 17475400 (D.D.C. Dec. 6, 2022).....	6, 7, 23
<i>Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.,</i> 511 U.S. 164 (1994).....	25, 26, 27, 28
<i>Cheng v. Boeing Co.,</i> 708 F.2d 1406 (9th Cir. 1983) .....	20
<i>Clagett v. Allstate Ins. Co.,</i> 71 Va. Cir. 105 (2006).....	29
<i>Consulting Eng'r's Corp. v. Geometric Ltd.,</i> 561 F.3d 273 (4th Cir. 2009) .....	11, 12
<i>Cook v. Champion Tankers AS,</i> 2013 WL 1629136 (N.D. Cal. Apr. 16, 2013) .....	21
<i>Corrie v. Caterpillar, Inc.,</i> 403 F. Supp. 2d 1019 (W.D. Wash. Nov. 22, 2005).....	16, 17
<i>CoStar Realty Info., Inc. v. Field,</i> 737 F. Supp. 2d 496 (D. Md. 2010) .....	23
<i>Daimler AG v. Bauman,</i> 571 U.S. 117 (2014).....	8

<i>DHI Grp. v. Kent,</i> 2017 WL 1088352 (S.D. Tex. Mar. 3, 2017).....	26
<i>Doğan v. Barak,</i> 932 F.3d 888 (9th Cir. 2019) .....	7
<i>DTC Energy Grp. v. Hirschfeld,</i> 420 F. Supp. 3d 1163 (D. Colo. 2019).....	25
<i>Du Daobin v. Cisco Sys.,</i> 2 F. Supp. 3d 717 (D. Md. 2014).....	14, 15, 16
<i>Estate Constr. Co. v. Miller &amp; Smith Holding Co.,</i> 14 F.3d 213 (4th Cir. 1994) .....	25
<i>In re Factor VIII or IX Concentrate Blood Prods. Liab. Litig.,</i> 2008 WL 4866431 (N.D. Ill. June 4, 2008).....	18
<i>Fahrner-Miller Assocs., Inc. v. Mars Antennas &amp; RF Sys., Ltd.,</i> 2014 WL 6871550 (N.D. Cal. Dec. 4, 2014).....	16
<i>Farrar v. McFarlane Aviation, Inc.,</i> 823 F. App'x 161 (4th Cir. 2020) .....	10
<i>Fed. Ins. Co. v. Lake Shore Inc.,</i> 886 F.2d 654 (4th Cir. 1989) .....	12
<i>Fidrych v. Marriott Int'l, Inc.,</i> 952 F.3d 124 (4th Cir. 2020) .....	8, 10, 11
<i>Flynn v. Liner Grode Stein Yankelevitz Sunshine Regenstreif &amp; Taylor LLP,</i> 2011 WL 2847712 (D. Nev. July 15, 2011) .....	26
<i>Freeman v. DirecTV, Inc.,</i> 457 F.3d 1001 (9th Cir. 2006) .....	26
<i>Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.,</i> 284 F.3d 1114 (9th Cir. 2002) .....	12
<i>Global Policy Partners, LLC v. Yessin,</i> 686 F. Supp. 2d 642 (E.D. Va. 2010) .....	23
<i>Grizzard v. LG Chem Ltd.,</i> 641 F. Supp. 3d 282 (E.D. Va. 2022) .....	12
<i>GTE Wireless, Inc. v. Qualcomm, Inc.,</i> 71 F. Supp. 2d 517 (E.D. Va. 1999) .....	21

<i>Harris v. Kreutzer</i> , 271 Va. 188 (2006) .....	28
<i>Hawkins v. i-TV Digitalis Tavkozlesi zrt.</i> , 935 F.3d 211 (4th Cir. 2019) .....	10, 11, 13
<i>Henkin v. Islamic Rep. of Iran</i> , 2021 WL 2914036 (D.D.C. July 12, 2021).....	16, 17
<i>Herbage v. Meese</i> , 747 F. Supp. 60 (D.D.C. 1990).....	7
<i>Interface Partners Int'l Ltd. v. Hananel</i> , 575 F.3d 97 (1st Cir. 2009).....	16
<i>Israel Discount Bank Ltd. v. Schapp</i> , 505 F. Supp. 2d 651 (C.D. Cal. 2007) .....	16
<i>Ivey v. Lynch</i> , 2018 WL 3764264 (M.D.N.C. Aug. 8, 2018).....	7
<i>Jiali Tang v. Synutra Int'l, Inc.</i> , 656 F.3d 242 (4th Cir. 2011) .....	<i>passim</i>
<i>King v. City of Chesapeake</i> , 478 F. Supp. 2d 871 (E.D. Va. 2007) .....	29
<i>Koninklijke Philips N.V. v. Elec-Tech Int'l Co.</i> , 2015 WL 1289984 (N.D. Cal. Mar. 20, 2015).....	24
<i>La Casa Real Estate &amp; Inv., LLC v. KB Home of S.C., Inc.</i> , 2010 WL 2649867 (M.D.N.C. June 30, 2010) .....	20
<i>M.A. v. INS</i> , 899 F.2d 304 (4th Cir. 1990) .....	14
<i>MGA Ent. Inc. v. Deutsche Bank AG</i> , 2012 WL 12892902 (C.D. Cal. Feb. 27, 2012).....	19
<i>Moriah v. Bank of China Ltd.</i> , 107 F. Supp. 3d 272 (S.D.N.Y. 2015).....	7
<i>NetApp, Inc. v. Nimble Storage, Inc.</i> , 2015 WL 400251 (N.D. Cal. Jan. 29, 2015) .....	22, 25
<i>OSI Sys., Inc. v. KM-Logix, LLC</i> , 2022 WL 2292725 (E.D. Va. June 24, 2022) .....	23, 29, 30

<i>Pediatric Nephrology Assocs. of S. Fla. v. Variety Children's Hosp.,</i> 226 F. Supp. 3d 1346 (S.D. Fla. 2016) .....	22
<i>Phreesia, Inc. v. Certify Global, Inc.,</i> 2022 WL 911207 (D. Md. Mar. 29, 2022).....	22, 23, 24
<i>Piper Aircraft Co. v. Reyno,</i> 454 U.S. 235 (1981), and NSO .....	17, 21
<i>Podium Corp. Inc. v. Chekkit Geolocation Servs., Inc.,</i> 2021 WL 5772269 (D. Utah Dec. 6, 2021).....	26
<i>Return Mail, Inc. v. USPS,</i> 139 S. Ct. 1853 (2019).....	27
<i>Riot Games, Inc. v. Shanghai Moonton Tech. Co.,</i> 2022 WL 17326150 (C.D. Cal. Nov. 8, 2022).....	20
<i>Rishikof v. Mortada,</i> 70 F. Supp. 3d 8 (D.D.C. 2014).....	7
<i>Rubin v. Islamic Rep. of Iran,</i> 637 F.3d 783 (7th Cir. 2011) .....	18
<i>Russo v. White,</i> 241 Va. 23 (1991) .....	28
<i>Sarei v. Rio Tinto, PLC,</i> 550 F.3d 822 (9th Cir. 2008) .....	14
<i>Saudi Arabia v. Nelson,</i> 507 U.S. 349 (1993).....	15, 24, 27, 29
<i>SecureInfo Corp. v. Telos Corp.,</i> 387 F. Supp. 2d 593 (E.D. Va. 2005) .....	30
<i>Sherley v. Lotz,</i> 200 Va. 173 (1958) .....	27
<i>Sinochem Int'l Co. v. Malaysia Int'l Shipping,</i> 549 U.S. 422 (2007).....	16
<i>St. Jarre v. Heidelberger Druckmaschinen, A.G.,</i> 19 F.3d 1430 .....	12
<i>State Analysis, Inc. v. Am. Fin. Servs. Ass'n,</i> 621 F. Supp. 2d 309 (E.D. Va. 2009) .....	24

<i>Supervalu, Inc. v. Johnson</i> , 276 Va. 356 (2008) .....	28
<i>United States v. Burgos</i> , 94 F.3d 849 (4th Cir. 1996) .....	26
<i>Van Buren v. United States</i> , 141 S. Ct. 1648 (2021).....	22, 23
<i>Velasco v. Gov't of Indonesia</i> , 370 F.3d 398 (4th Cir. 2004) .....	7
<i>W. Union Telegraph Co. v. Davis</i> , 114 Va. 154 (1912) .....	27
<i>Walden v. Fiore</i> , 571 U.S. 277 (2014).....	10, 11
<i>Westwind Acquisition Co. v. Universal Weather &amp; Aviation, Inc.</i> , 668 F. Supp. 2d 749 (E.D. Va. 2009) .....	27
<i>WhatsApp Inc. v. NSO Grp. Techs. Ltd.</i> , 472 F. Supp. 3d 649 (N.D. Cal. 2020) .....	16, 24, 27
<i>Wilson v. ImageSat Int'l N.V.</i> , 2008 WL 2851511 (S.D.N.Y. July 22, 2008) .....	16
<i>Wynne v. I.C. Sys., Inc.</i> , 124 F. Supp. 3d 734 (E.D. Va. 2015) .....	27
<i>Yousuf v. Samantar</i> , 699 F.3d 763 (4th Cir. 2012) .....	7
<b>Statutes and Regulations</b>	
18 U.S.C. 1030(e)(11).....	23
18 U.S.C. 1030(g) .....	24
18 U.S.C. § 1030.....	26
18 U.S.C. § 1030(b) .....	25
18 U.S.C. § 1030(c)(4)(A)(i)(I) .....	23
18 U.S.C. § 1030(e)(8).....	22
28 U.S.C. § 1604.....	7, 18

Va. Code § 18.2-152.2 .....	27
Va. Code § 18.2-152.4 .....	27
Va. Code § 18.2-152.12 .....	27
15 C.F.R. § 734.3(a)(1).....	4
15 C.F.R. § 772.1 .....	4
15 C.F.R. § 744, Supp. 4.....	4, 20
15 C.F.R. § 744.11(a).....	20

## **Other Authorities**

Dov Lieber et al., <i>Police Tracked a Terror Suspect—Until His Phone Went Dark After a Facebook Warning</i> , Wall St. J. (Jan. 2, 2020, 3:29 p.m.).....	2
Eddy Meiri, <i>Foreign Judgments Enforcement in Israel</i> , 31 Int'L. Practicum 39 (2018).....	19
NSO Group, <i>Transparency and Responsibility Report 2021</i> (June 30, 2021), <a href="https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf">https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf</a> .....	2, 3
Peter Nash Swisher et al., Va. Prac. Tort and Personal Injury Law .....	29
Stephanie Kirchgaessner, <i>Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests</i> , Guardian (July 18, 2021) .....	6

## **MEMORANDUM OF POINTS AND AUTHORITIES**

### **INTRODUCTION**

Plaintiff sues NSO for alleged actions that, under her own Complaint, were committed solely by the United Arab Emirates on behalf of Saudi Arabia. NSO condemns the killing of Jamal Khashoggi in the strongest terms. But NSO was not involved in any of the allegedly unlawful conduct described in Plaintiff's complaint, and NSO cannot be sued for that alleged conduct in this Court. Because Plaintiff challenges actions that she alleges were taken by or on behalf of Saudi Arabia and the UAE, foreign sovereign immunity deprives this Court of subject-matter jurisdiction. The act of state doctrine bars Plaintiff's claims for the same reason. And because NSO is a foreign company whose alleged conduct occurred overseas, it is not subject to personal jurisdiction in Virginia, and this Court is an inappropriate forum under the doctrine of *forum non conveniens*.

In addition to these categorical bars to her suit, Plaintiff does not adequately plead any of her claims. She does not state a claim against NSO under the Computer Fraud and Abuse Act ("CFAA") because she does not allege NSO committed any of the alleged acts that violated the CFAA. Her state-law tort claims all fail because Virginia law does not and cannot apply to NSO's purely foreign alleged conduct. Even if Virginia law could apply, Plaintiff does not plead sufficient facts to establish that NSO violated the Virginia Computer Crimes Act ("VCCA"), owed Plaintiff any duty of care, negligently or intentionally inflicted severe emotional distress on Plaintiff, or trespassed to any chattel of Plaintiff's.

For these reasons, all of Plaintiff's claims should be dismissed.

### **BACKGROUND**

#### **A. NSO's technology and its use in preventing terrorism and other crimes.**

Defendant NSO is an Israeli technology company that designs, markets, and licenses—exclusively to foreign governments—a highly regulated technology used to investigate and prevent terrorism and serious crimes. (Shohat Decl. ¶¶ 3-4, 6-12; Compl. ¶ 20.) Defendant Q Cyber, also an Israeli company, is NSO's shareholder. (Shohat Decl. ¶ 4; Compl. ¶¶ 21-22.) The export of NSO's "Pegasus" technology is regulated under Israel's Defense Export Control Law ("DECL"),

and the Israeli Ministry of Defense determines the government agencies to which NSO may market or license its technology. (Shohat Decl. ¶¶ 6-9 & Exh. A.)

NSO does not operate its Pegasus technology. Instead, it licenses the technology to foreign government agencies and provides training, setup, and installation of the technology. (*Id.* ¶ 11; *see* Compl. ¶¶ 36, 44.) NSO's government customers—not NSO—operate the technology and make all decisions about how to do so. (Shohat Decl. ¶ 11.)<sup>1</sup> NSO has no knowledge of who any customer monitors using NSO's technology and does not have access to any information gathered by its customers. (*Id.* ¶ 14.) But NSO designs its technology to be used solely to prevent and investigate terrorism and other serious crimes—no different than investigatory wiretaps lawfully used by the United States and other Western democracies.<sup>2</sup> Governments and government agencies have successfully used NSO's technology to thwart major terrorist attacks, identify and capture child sex abusers, break up criminal organizations and drug trafficking rings, and free kidnapping and human trafficking victims.<sup>3</sup>

NSO's license agreements prohibit its government customers from using the technology against anyone who is not a suspected terrorist or criminal. (*Id.*) If a government ever misused the technology to monitor anyone other than suspected criminals or terrorists, that would be a violation of that government's contract with NSO. (*Id.*) NSO contractually can suspend and/or terminate service to customers engaged in any improper use of NSO's Pegasus technology—and has done so. (*Id.*) In addition, NSO has voluntarily undertaken additional steps to ensure that its Pegasus

---

<sup>1</sup> The alleged misuses of Pegasus alleged in Plaintiff's Complaint are irrelevant to her claims, but she claims they were all committed by foreign governments, not by NSO. (*See* Compl. ¶ 57 ("[NSO's] clients"); *id.* ¶ 63 ("Mexican Government"); *id.* ¶ 74 ("UAE Government"); *id.* ¶ 80 ("Rwandan government"); *id.* ¶ 83 ("Ghanaian government").

<sup>2</sup> *See, e.g.*, Dov Lieber et al., *Police Tracked a Terror Suspect—Until His Phone Went Dark After a Facebook Warning*, Wall St. J. (Jan. 2, 2020, 3:29 p.m.), <https://on.wsj.com/38uXk5s> (discussing European democracies' use of NSO's technology to investigate Islamic State terrorists).

<sup>3</sup> NSO Group, *Transparency and Responsibility Report 2021* at 7 (June 30, 2021), <https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf> ("NSO Transparency Report").

technology is used responsibly by authorized public safety authorities.<sup>4</sup> NSO takes into account U.S. and European Union export control restrictions in addition to Israel’s DECL. (*Id.* ¶ 12.) It has committed itself to the authoritative international standards of the United Nations’ Guiding Principles on Business and Human Rights and the Organization for Economic Cooperation and Development’s Guidelines for Multinational Enterprises.<sup>5</sup> Consistent with those standards, NSO conducts due diligence on all potential customers, examining publicly available information, rule-of-law considerations, questionnaires, and other items. (*Id.*) Government customers are contractually required to provide these due diligence materials before receiving NSO technology. (*Id.*)

**B. Export control regulation of NSO’s operations.**

NSO’s activities with respect to Pegasus are “strictly monitored and regulated by the Government of Israel.” (*Id.* ¶ 6.) Israel’s DECL prohibits the transfer of “defense know how,” such as information about Pegasus, outside of Israel unless the Israeli government grants a license. (*Id.* ¶ 7 & Exh. A.) The licensing and oversight process involves the exchange of documents and information with the Israeli Ministry of Defense, including information about NSO’s prospective customers, information about the technology requested for export, the intended uses of Pegasus (to confirm that the technology will only be used for law enforcement and antiterrorism purposes), and investigations into potential misuses of the technology. (*Id.* ¶¶ 7-11.) Under Israel’s DECL, the Israeli Ministry of Defense may investigate NSO and its business and refuse or cancel NSO’s registration. (*Id.* ¶ 7.) The Ministry of Defense is also authorized to grant or deny NSO’s licenses, taking into account factors such as the intended use of NSO’s technology and the identity of its customers, and it also has authority to revoke NSO’s licenses entirely. (*Id.*; DECL Ch. C (3-4).)

On July 19, 2020, [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED] (Blecher Decl. ¶ 3.)

---

<sup>4</sup> See NSO Transparency Report at 8-30.

<sup>5</sup> NSO Transparency Report at 8.

[REDACTED]  
[REDACTED] (Id. ¶ 4 & Exh. A.) The same day, [REDACTED]

[REDACTED] (Id. ¶ 5 & Exh. B.)

[REDACTED] (Id. Exh. B at 1.) [REDACTED]

[REDACTED].<sup>6</sup> (Id.) [REDACTED]  
[REDACTED] (Id. ¶ 6.)

Separately, on November 4, 2021, the U.S. Department of Commerce restricted U.S. exports to NSO. *See* 15 C.F.R. § 744, Supp. 4. The Department’s Bureau of Industry and Security (“BIS”) entered the “NSO Group” on its Entity List, which prohibits any U.S. entity from exporting to NSO items subject to Export Administration Regulations. *See id.* (Compl. ¶ 43). Under the regulations, “items” include hardware, software, technology, and related technical information that is currently located in—or comes into—the United States. 15 C.F.R. §§ 734.3(a)(1), 772.1. BIS may grant licenses authorizing the transfer of items to NSO subject to the regulations, but it indicated that licenses regarding NSO would be subject to a presumption of denial. *Id.* § 744, Supp. 4.

In early 2023, NSO and its defense counsel sought export licenses from the Israeli and U.S. governments. On February 21, 2023, King & Spalding applied to BIS for an export license. (Akro. Decl. ¶ 2.) The license was intended to permit King & Spalding to discuss with NSO information about NSO’s technology, as well as similar items and information received from third parties, so that King & Spalding could prepare NSO’s defense in litigation. (Id.) The license application was returned without action on April 20, 2023. (Id.) Subsequent discussions with BIS have not resulted in a license being granted. (Id.) On June 8, 2023, NSO applied to the Israeli Ministry of Defense for a license to export certain information relating to Pegasus. (Shohat Decl. ¶ 17.) To date, the

---

<sup>6</sup> [REDACTED]

[REDACTED] (Blecher Decl. ¶ 7.)

Ministry has not granted the requested license. (*Id.*)

(Blecher Decl. ¶ 8 & Exh. C [REDACTED]

[REDACTED] First, [REDACTED]

[REDACTED] (*Id.* Exh. C ¶ 3.)

Second, NSO [REDACTED]

(*Id.* ¶ 4.) Third, NSO [REDACTED]

[REDACTED] (*Id.* ¶ 5.) Furthermore, [REDACTED]

### **C. Plaintiff and her allegations.**

Plaintiff claims she was targeted for monitoring by Saudi Arabia and the UAE because of her relationship to Jamal Khashoggi. She alleges NSO licensed its Pegasus technology to the UAE, which then worked with Saudi Arabia to misuse the technology and monitor Plaintiff's private communications. Specifically, Plaintiff alleges that "an agency of the UAE" sent her "a text message" containing "a disabled Pegasus link." (Compl. ¶ 102.) Because the link was "disabled," Plaintiff does not allege that Pegasus was *installed* on any of her devices as a result of the UAE's

<sup>7</sup>

[REDACTED] (Blecher Decl. ¶ 8 & Exh. D.)

[REDACTED] (*Id.* Exh. D ¶ 2(1)-(6).)

(a)-(b.).

[REDACTED] (*Id.* ¶ 4

text messages.<sup>8</sup> Instead, she alleges she was later “detained” by “Emirati intelligence officers” who “manually installed” Pegasus “onto at least one of her phones.” (Compl. ¶ 106.) Plaintiff alleges the UAE did this to assist its “key ally,” the “Kingdom of Saudi Arabia,” with persecution of Mr. Khashoggi. (Compl. ¶ 108.) Plaintiff does not allege any facts suggesting that NSO had any involvement in any government’s alleged use of NSO’s Pegasus technology.

In October 2018, Mr. Khashoggi traveled to the Saudi consulate in Istanbul, Turkey, to receive documentation necessary to marry his fiancée, Hatice Cengiz. *Cengiz v. Salman*, 2022 WL 17475400, at \*4-7 (D.D.C. Dec. 6, 2022). Saudi officials knew Mr. Khashoggi would be at the Istanbul consulate because he had informed them that he would be travelling there. *Id.* While Mr. Khashoggi was at the consulate, Saudi agents—“assisted by allies in the [UAE]”—allegedly kidnapped and murdered him. (Compl. ¶¶ 4, 117, 120-21.) Plaintiff does not allege any facts suggesting that Saudi Arabia’s and the UAE’s alleged misuse of Pegasus had any causal connection to Mr. Khashoggi’s murder. NSO strongly condemns Mr. Khashoggi’s killing, which goes against everything NSO stands for. (Compl. ¶ 122.)

## ARGUMENT

### I. THE COURT SHOULD DISMISS BECAUSE IT LACKS AUTHORITY TO ADJUDICATE THIS CASE.

#### A. The Court lacks subject-matter jurisdiction because NSO is entitled to derivative foreign sovereign immunity.

Plaintiff is suing NSO because she cannot sue a foreign state. Plaintiff’s allegations clearly challenge the conduct of the UAE and Saudi Arabia. According to Plaintiff, it was the UAE (acting on Saudi Arabia’s behalf) that allegedly installed Pegasus on Plaintiff’s devices and monitored Plaintiff’s private communications. (E.g., Compl. ¶¶ 102-113.) But because the UAE and Saudi

---

<sup>8</sup> According to public reporting incorporated into Plaintiff’s complaint, “[a] forensic analysis of [her] Android phone ... did not confirm whether the device had been successfully infected.” Stephanie Kirchgaessner, *Saudis Behind NSO Spyware Attack on Jamal Khashoggi’s Family, Leak Suggests*, Guardian (July 18, 2021), <https://tinyurl.com/3fms4j32> (cited at Compl. ¶ 122 n.60).

Arabia are foreign states, the Foreign Sovereign Immunities Act (“FSIA”) deprives federal courts of jurisdiction over a suit by Plaintiff against either. 28 U.S.C. § 1604.<sup>9</sup> Plaintiff’s suit against NSO is therefore an attempt to end-run the FSIA. That is improper. Because Plaintiff alleges that NSO acted on behalf of Saudi Arabia and the UAE to assist those nations’ sovereign activities, NSO is immune. This Court lacks jurisdiction over Plaintiff’s claims.

While the FSIA immunizes only foreign states, common-law foreign sovereign immunity “extend[s] to an individual acting in his official capacity on behalf of a foreign state.” *Velasco v. Gov’t of Indonesia*, 370 F.3d 398, 399 (4th Cir. 2004); *accord Yousuf v. Samantar*, 699 F.3d 763, 769 (4th Cir. 2012); *Doğan v. Barak*, 932 F.3d 888, 893-94 (9th Cir. 2019); *Rishikof v. Mortada*, 70 F. Supp. 3d 8, 13 (D.D.C. 2014); *Herbage v. Meese*, 747 F. Supp. 60, 66 (D.D.C. 1990). The Fourth Circuit has held that even *private* actors are derivatively immune when they act on behalf of foreign governments. *Butters v. Vance Int’l, Inc.*, 225 F.3d 462, 466 (4th Cir. 2000).

*Butters* governs here. The plaintiff in *Butters* was a bodyguard whose employer had been hired by Saudi Arabia to protect its princess. At Saudi Arabia’s request, the employer did not promote the plaintiff, who sued the employer. The Fourth Circuit held that the employer was derivatively immune as the “private agent[] of [a] foreign government.” *Id.* Other courts, before and after *Butters*, have reached the same conclusion. *See Ivey v. Lynch*, 2018 WL 3764264, at \*6 (M.D.N.C. Aug. 8, 2018) (following *Butters* to find private agent of foreign official immune); *Moriah v. Bank of China Ltd.*, 107 F. Supp. 3d 272, 277 & n.34 (S.D.N.Y. 2015) (holding based on *Butters* that common-law immunity “extends beyond current and former government officials to individuals acting as an agent for the government”); *Alicog v. Kingdom of Saudi Arabia*, 860 F. Supp. 379, 384 (S.D. Tex. 1994), *aff’d*, 79 F.3d 1145 (5th Cir. 1996) (holding agents enjoy immunity when acting on behalf of foreign government).

NSO is entitled to derivative foreign sovereign immunity under *Butters*. Plaintiff alleges

---

<sup>9</sup> The United States filed a suggestion of immunity in a lawsuit filed against the Crown Prince of Saudi Arabia by Hatice Cengiz. The district court dismissed Ms. Cengiz’s claims based on the United States’ suggestion of immunity. *Cengiz*, 2022 WL 17475400, at \*4-7.

the UAE monitored her devices on behalf of Saudi Arabia and did so using NSO’s technology. (E.g., Compl. ¶ 101-03, 106-08, 113.) But she cannot deny that “a foreign government’s deployment of clandestine agents to collect foreign intelligence on its behalf” is “peculiarly sovereign conduct” for which foreign governments are immune from suit. *Broidy Cap. Mgmt., LLC v. Qatar*, 982 F.3d 582, 595 (9th Cir. 2020). While Plaintiff’s factual allegations are conspicuously silent on what, if anything, NSO allegedly did after licensing its technology to the UAE,<sup>10</sup> her complaint is clear that any claimed actions would have been taken on behalf of the UAE or Saudi Arabia. (Cf. Compl. ¶ 45 (alleging generally that NSO “assist[s]” its clients); *id.* ¶ 66 (alleging generally that NSO “offers four levels of support to its clients after selling Pegasus to them”)). Indeed, Plaintiff alleges that her “private communications” were intercepted “by agents of an authoritarian government.” (Compl. ¶ 129 (emphasis added).)

Plaintiff does not allege that NSO took any case-related action against her that was not conducted in its alleged role as an agent of the UAE or Saudi Arabia. NSO is therefore entitled to derivative foreign sovereign immunity as an alleged “private agent[] of [a] foreign government.” *Butters*, 225 F.3d at 466.

#### **B. The Court lacks personal jurisdiction over NSO.**

Even if the Court had subject-matter jurisdiction, NSO is not subject to personal jurisdiction in Virginia.

##### **1. NSO is not subject to personal jurisdiction in Virginia.**

General jurisdiction exists only when a defendant’s contacts with the forum state “are so constant and pervasive as to render it essentially at home” there. *Daimler AG v. Bauman*, 571 U.S. 117, 122 (2014) (cleaned up). In all but the rare “exceptional case,” a corporation is “at home” only in its place of incorporation and principal place of business. *Fidrych v. Marriott Int’l, Inc.*,

---

<sup>10</sup> To be clear, NSO *was not involved* in any monitoring of Plaintiff. But to the extent Plaintiff alleges otherwise, she treats NSO as an agent of Saudi Arabia and the UAE.

952 F.3d 124, 133 (4th Cir. 2020). NSO is not subject to general jurisdiction in Virginia because it is incorporated and has its principal place of business in Israel. (Compl. ¶¶ 20-22.)

In the absence of general jurisdiction, Plaintiff must establish specific jurisdiction by alleging facts showing that her “claims arise out of” activities by which NSO “purposefully availed itself of the privilege of conducting activities in” Virginia. *Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.*, 334 F.3d 390, 397 (4th Cir. 2003). In a case like this, in which Plaintiff bases her claims on alleged “Internet-based” conduct, Plaintiff must establish that NSO “acted with the ‘manifest intent’ of targeting” Virginia. *Id.* at 399-400.

Plaintiff cannot do so. She asserts that NSO “intentionally target[ed] … her devices in Virginia” (Compl. ¶ 30), but she pleads no facts to support that conclusory assertion.<sup>11</sup> She does not even clearly allege that any access occurred in Virginia. She alleges the UAE sent her a “text message” containing a “disabled Pegasus link” in November 2017 (Compl. ¶ 102), but she does not allege she lived in Virginia at that time. She alleges only that Jamal Khashoggi “invited her to reconnect with him in his new home in Virginia” at some unspecified time after “the summer of 2017.” (Compl. ¶ 12.) Indeed, elsewhere in the Complaint, she suggests that she did not “flee[] to the United States” until *after* “the Pegasus attacks.” (Compl. ¶ 145.) The UAE’s alleged manual installation of Pegasus on Plaintiff’s phone allegedly occurred in the UAE, not in Virginia. (Compl. ¶ 106.) Plaintiff’s failure to clearly allege that Pegasus was ever installed or used on her phone in Virginia is not surprising, since Pegasus *cannot* be used in the United States or on U.S. devices. (Shohat Decl. ¶ 13.)

Even more important, Plaintiff does not allege any Virginia-related conduct by NSO—the only potentially relevant conduct she describes was allegedly committed solely by Saudi Arabia

---

<sup>11</sup> Similarly, Plaintiff’s CFAA cause of action alleges that “Defendants” accessed her devices (Compl. ¶¶ 135-141), but those are merely conclusory recitations of the CFAA’s elements. Plaintiffs’ factual allegations provide no support for those assertions. See *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (“Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.”).

or the UAE. She alleges “Saudi Arabia … leveraged its relationship with a key ally, the United Arab Emirates, to install Pegasus on her phones.” (Compl. ¶ 108.) She alleges the “text message” with a “disabled Pegasus link” was sent by “an agency of the UAE.” (Compl. ¶ 102.) She alleges Pegasus was “manually installed” in the UAE by “Emirati intelligence officers.” (Compl. ¶ 106 & n.54.) And she alleges her private communications were “relayed to the Saudis, via the UAE” (Compl. ¶ 113), and “invaded by agents of an authoritarian government” (Compl. ¶ 129).

Plaintiffs’ allegations that *Saudi Arabia and the UAE* targeted her devices cannot support specific jurisdiction *over NSO*. To create specific jurisdiction, “[t]he connection between the defendant and the forum must arise out of contacts that the defendant *himself* creates with the forum State.” *Fidrych*, 952 F.3d at 143 (internal quotation marks omitted). “[I]t is the defendant, not the plaintiff or third parties, who must create contacts with the forum State.” *Walden v. Fiore*, 571 U.S. 277, 291 (2014). Although Plaintiff may not “satisfy the defendant-focused ‘minimum contacts’ inquiry by demonstrating contacts between … third parties[] and the forum state,” *id.* at 284, those are the only allegations included in her Complaint.

The limited conduct Plaintiff attributes to NSO has no connection to Virginia. Plaintiff alleges that NSO licensed its Pegasus technology to the UAE, but that would have occurred entirely overseas. NSO did not allegedly “direct[] purposeful activity toward [Virginia] in relation to those particular sales.” *Farrar v. McFarlane Aviation, Inc.*, 823 F. App’x 161, 164 (4th Cir. 2020). Plaintiff does not allege NSO had any involvement in Saudi Arabia’s and the UAE’s supposed decision to misuse Pegasus to monitor Plaintiff. Even if she did, “the mere act of aiding and abetting is not always enough to provide minimum contacts” because “aiding-and-abetting … does not necessarily involve the sort of ‘express aiming’ at the forum that the effects test requires.” *Hawkins v. i-TV Digitalis Tavkozlesi zrt.*, 935 F.3d 211, 230-31 (4th Cir. 2019). Plaintiff alleges no facts suggesting that NSO had any “control over” Saudi Arabia’s and the UAE’s alleged decisions to monitor Plaintiff. *Farrar*, 823 F. App’x at 164.

Plaintiff does not even allege NSO knew Saudi Arabia or the UAE would allegedly use

Pegasus to monitor Plaintiff—or any other Virginia resident.<sup>12</sup> Such knowledge, even if alleged, would not support specific jurisdiction. *Walden*, 571 U.S. at 289. A “person cannot be haled into court in a forum simply because he knew that his conduct would have incidental effects there; he must have ‘expressly aimed’ his conduct at the forum.” *Hawkins*, 935 F.3d at 230. And “mere knowledge of an incidental in-forum effect falls short of express aiming.” *Id.* at 231. Because Plaintiff does not allege facts showing that NSO played any direct role in accessing or monitoring her devices in Virginia, her factual allegations do not plausibly “suggest[]” that NSO “aimed [its] conduct at Virginia or, more broadly, the United States as a whole.” *Id.*

“This conclusion finds support in the serious comity concerns that would arise if [the Court] permitted the exercise of personal jurisdiction over foreign nonparties based on purely foreign conduct.” *Id.* NSO is an Israeli corporation, and Plaintiff is suing it because it allegedly licensed its technology to a foreign country that allegedly misused the technology to monitor Plaintiff. But NSO’s only alleged role in that conduct—its Israel-approved decision to license its technology to the UAE—occurred overseas and had no connection to Virginia. “[O]ther nations would surely look askance at us if a mere allegation of aiding-and-abetting, occurring entirely overseas, sufficed to provide our courts with jurisdiction over their citizens.” *Id.* This Court cannot exercise specific jurisdiction over NSO based on Plaintiff’s allegations of foreign conduct.

## 2. Exercising personal jurisdiction over NSO would be unreasonable.

Separate from the “minimum contacts” analysis, due process requires that a court’s exercise of specific jurisdiction “be constitutionally reasonable.” *Consulting Eng’rs Corp. v. Geometric Ltd.*, 561 F.3d 273, 278 (4th Cir. 2009). Under that requirement, courts “consider additional factors to ensure the appropriateness of the forum,” including “(1) the burden on the defendant of litigating in the forum; (2) the interest of the forum state in adjudicating the dispute;

---

<sup>12</sup> Plaintiff’s current Virginia residence cannot itself support specific jurisdiction. *Walden*, 571 U.S. at 289. “Put simply, however significant the plaintiff’s contacts with the forum may be, those contacts *cannot be decisive* in determining whether the defendant’s due process rights are violated.” *Fidrych*, 952 F.3d at 143 (quoting *Walden*, 571 U.S. at 285).

(3) the plaintiff's interest in obtaining convenient and effective relief; (4) the shared interest of the states in obtaining efficient resolution of disputes; and (5) the interests of the states in furthering substantive social policies." *Id.* at 279.

Here, these factors demonstrate that exercising personal jurisdiction over NSO would not be reasonable. Plaintiff does not allege that NSO, as opposed to Saudi Arabia and the UAE, took any intentional action aimed at Virginia. *See St. Jarre v. Heidelberger Druckmaschinen, A.G.*, 19 F.3d 1430 (Table), at \*3 (4th Cir. 1994) ("The exercise of personal jurisdiction over a foreign manufacturer, whose product reached the forum state because of intervening sales by third parties, would be unfair and unreasonable."). And the "burden" on NSO of litigating this suit in Virginia "would be considerable." *Fed. Ins. Co. v. Lake Shore Inc.*, 886 F.2d 654, 661 (4th Cir. 1989). NSO "is incorporated in [Israel], owns no property in the forum, and has no employees or persons authorized to act on its behalf there." *Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.*, 284 F.3d 1114, 1125–26 (9th Cir. 2002). It has no evidence or witnesses in Virginia (Shohat Decl. ¶¶ 5, 16), and most of the "witnesses and evidence relevant to [Plaintiff's] claims are located" in Israel, Saudi Arabia, and the UAE. *Fed. Ins.*, 886 F.2d at 661. The Israeli DECL [REDACTED] [REDACTED], along with NSO's presence on the Entity List, will impose substantial restrictions on discovery in this action and impair NSO's ability to defend itself. Although Plaintiff currently resides in Virginia, she does not allege facts showing that she "fle[d] to the United States" (Compl. ¶ 145) or even lived in the United States when her devices were allegedly accessed. In any event, her "convenience alone cannot justify the heavy burden on [NSO] which the assertion of personal jurisdiction would impose." *Id.*; *see Grizzard v. LG Chem Ltd.*, 641 F. Supp. 3d 282, 292 (E.D. Va. 2022) (finding jurisdiction unreasonable even though "a number of ... factors may point in [p]laintiff's favor" because "[d]ue process limits on the State's adjudicative authority principally protect the liberty of the nonresident defendant—not the convenience of the plaintiffs or third parties" (quoting *Walden*, 571 U.S. at 284)).

Exercising personal jurisdiction over NSO in Virginia would also be unreasonable because it would interfere with the sovereignty of foreign nations. The Supreme Court has warned that

“great care and reserve should be exercised when extending our notions of personal jurisdiction into the international field.” *Asahi Metal Indus. Co. v. Super. Ct.*, 480 U.S. 102, 115 (1987) (cleaned up). “Where, as here, the defendant is from a foreign nation rather than another state, the sovereignty barrier is high and undermines the reasonableness of personal jurisdiction.” *Amoco Egypt Oil Co. v. Leonis Nav. Co.*, 1 F.3d 848, 852 (9th Cir. 1993); *see also Hawkins*, 935 F.3d at 232 (considering “comity concerns” when rejecting personal jurisdiction). As noted above, Plaintiff challenges actions allegedly conducted or ordered by Saudi Arabia and the UAE, so exercising jurisdiction would interfere with those countries’ sovereignty as well. *See Alhathloul v. DarkMatter Grp.*, 2023 WL 2537761, at \*10 (D. Or. Mar. 16, 2023) (finding personal jurisdiction unreasonable because plaintiff’s “claims ‘relate to conduct carried out at the behest of the UAE government’”). Moreover, this lawsuit in particular poses severe threats to Israel’s sovereignty because Israel regulates and reviews NSO’s operations—including the licensing decisions that Plaintiff seeks to challenge under Virginia law—and details of Israel’s decisions would have to be disclosed for NSO to defend this action. (Shohat Decl. ¶¶ 6-11, 16.)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The Israeli DECL likewise reflects a strong national-security interest in the subject-matter of this action, and it prohibits NSO from disclosing in this action broad swaths of information relevant to refuting Plaintiff’s claims. (Shohat Decl. ¶¶ 6-7 & Exh. A.)

### 3. NSO is not subject to jurisdiction under Rule 4(k)(2).

As a fallback to specific jurisdiction in Virginia, Plaintiff claims nationwide jurisdiction exists under Rule 4(k)(2). (Compl. ¶ 37.) But just as Plaintiff’s allegations do not “suggest[]” that NSO “aimed [its] conduct at Virginia,” they also do not suggest that NSO targeted “the United States as a whole.” *Hawkins*, 935 F.3d at 231. Plaintiff does not allege that NSO ever accessed or monitored any U.S. device or that its purely foreign conduct in licensing technology to foreign countries involved any purposeful direction toward the United States. Rule 4(k)(2) also cannot be

used to support personal jurisdiction over Plaintiff's state-law claims because, under Rule 4(k)(2), the plaintiff's claim must "arise under federal law." Fed. R. Civ. P. 4(k)(2).

Moreover, exercising personal jurisdiction over NSO in the United States would be unreasonable for the same reasons that it is unreasonable in Virginia. Jurisdiction under Rule 4(k)(2) is improper for that reason as well.

**C. The act of state doctrine bars Plaintiff's claims.**

The act of state doctrine provides an independent basis for dismissal, which the Court may address before reaching subject-matter or personal jurisdiction. *See Sarei v. Rio Tinto, PLC*, 550 F.3d 822, 824 n.1 (9th Cir. 2008). Under the act of state doctrine, "'when a court must decide ... the effect of official action by a foreign sovereign,' the court is precluded from considering the claim." *AdvanFort Co. v. Cartner*, 2015 WL 12516240, at \*5 (E.D. Va. Oct. 30, 2015) (quoting *W.S. Kirkpatrick & Co. v. Envtl. Tectonics Corp.*, 493 U.S. 400, 406 (1990)) (emphasis omitted); *see M.A. v. INS*, 899 F.2d 304, 314 (4th Cir. 1990); *Du Daobin v. Cisco Sys.*, 2 F. Supp. 3d 717, 726 (D. Md. 2014). The act of state doctrine applies, at a minimum, when "(1) the act undertaken by the foreign state was public; and (2) the act was completed within the sovereign's territory." *AdvanFort*, 2015 WL 12516240, at \*6. "However, the act of state doctrine is a flexible rule; therefore, a court could still apply the doctrine even if these two elements are not satisfied." *Id.* In particular, "the fact that a government entity acted outside the physical boundaries of the sovereign will not automatically defeat the doctrine's application where the decision ... is 'governmental' in nature." *Id.* at \*7.

The act of state doctrine bars Plaintiff's claims because they would require this Court to hold that governmental actions allegedly taken by Saudi Arabia and the UAE violated U.S. law. The basis of Plaintiff's claims is that the UAE allegedly misused NSO's technology to monitor her as part of Saudi Arabia's political crusade against Mr. Khashoggi. That alleged conduct, whether or not lawful under U.S. law, would have been undeniably "public" and "governmental." *AdvanFort*, 2015 WL 12516240, at \*5, 7. When "a foreign government[]" engages in "clandestine surveillance and espionage against a national of another nation in that other nation," it "employ[s] powers that—however controversial their status may be in international law—are peculiar to

sovereigns.” *Broidy*, 982 F.3d at 594 (internal quotation marks omitted); *see Saudi Arabia v. Nelson*, 507 U.S. 349, 361 (1993) (“[H]owever monstrous such abuse undoubtedly may be, a foreign state’s exercise of the power of its police has long been understood … as peculiarly sovereign in nature.”). Those governmental actions also occurred in foreign countries; the UAE allegedly installed Pegasus on Plaintiff’s phone in the UAE, and any actions by Saudi Arabia or the UAE in monitoring Plaintiff’s devices would have occurred within those nations’ borders. The location of Saudi Arabia’s or the UAE’s actions, however, is immaterial because of the “governmental” nature of their alleged conduct. *AdvanFort*, 2015 WL 12516240, at \*7 (holding act of state doctrine applied to governmental conduct “even if the pertinent acts occurred in Virginia”).

Plaintiff cannot avoid this result by challenging NSO’s alleged licensing of its technology to Saudi Arabia or the UAE. The licensing alone “entitle[s] Plaintiff[] to nothing under [her] theory of the case.” *Broidy*, 982 F.3d at 594 (cleaned up). Absent Saudi Arabia’s and the UAE’s alleged *use* of NSO’s technology, Plaintiff would have no cause of action. That aside, a nation’s purchase of surveillance technology is itself a governmental act; “a foreign government’s deployment of clandestine agents to collect foreign intelligence on its behalf,” even if conducted through “irregular operatives” such as private contractors, is “peculiarly sovereign conduct.” *Id.* at 595. In addition, the Government of Israel approves each license NSO issues for its technology. (Shohat Decl. ¶¶ 7, 11.) By challenging NSO’s licensing, Plaintiff necessarily challenges Israel’s governmental conduct in approving those licenses. The act of state doctrine applies for that reason as well. *See AdvanFort*, 2015 WL 12516240, at \*6-7 (holding act of state doctrine barred challenge to foreign government’s permitting decisions).

A court in this Circuit reached a similar conclusion in *Du Daobin*, 2 F. Supp. 3d at 725-26. There, the plaintiffs sued Cisco for allegedly designing and selling to China a “surveillance program” that China “used to detect, monitor, detain, suppress, and torture dissidents.” *Id.* at 720. The court held the act of state doctrine barred the lawsuit. Although the plaintiffs sued only Cisco for its conduct in designing and selling technology, their claims “effectively ask[ed] the [c]ourt to decide that the Chinese government, with substantial assistance from Cisco, has engaged in

multiple violations of international law.” *Id.* at 726. The act of state doctrine prohibited such “judicial interference” in the “official actions of the Chinese government and its officials.” *Id.*

The same rationale applies here, where Plaintiff challenges NSO’s design and sale of technology that successfully prevents terrorism and serious crimes because the UAE and Saudi Arabia allegedly misused that technology. Just like “the technology Cisco … allegedly customized and sold to China,” NSO’s technology “is inherently neutral technology that can clearly be used in a variety of non-offensive ways.” *Id.* at 725. Each of Plaintiff’s claims, however, “asks the Court to decide the extent to which apparently neutral technology can be used in other ways by foreign governments.” *Id.* The act of state doctrine forbids that result.

## **II. THE COMPLAINT SHOULD BE DISMISSED FOR *FORUM NON CONVENIENS*.**

Even if this Court enjoyed subject-matter and personal jurisdiction, the Complaint should still be dismissed under the doctrine of *forum non conveniens*. *See Sinochem Int’l Co. v. Malaysia Int’l Shipping*, 549 U.S. 422, 432 (2007). Dismissal is appropriate because, “when weighed against [P]laintiff’s choice of forum, the relevant public and private interests strongly favor” suit in Israel, an “adequate[] and available alternative forum.” *Jiali Tang v. Synutra Int’l, Inc.*, 656 F.3d 242, 246 (4th Cir. 2011) (internal quotation marks omitted).

### **A. Israel is an adequate alternative forum.**

“Courts routinely hold that Israel is a proper forum and dismiss cases on the grounds that it would be more appropriate to hear a case in Israel.” *Israel Discount Bank Ltd. v. Schapp*, 505 F. Supp. 2d 651, 659 (C.D. Cal. 2007) (citing cases).<sup>13</sup> Specifically, Israel is an adequate alternative forum for claims against NSO based on alleged uses of NSO’s technology. *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 677 (N.D. Cal. 2020). A foreign jurisdiction is available

---

<sup>13</sup> See also, e.g., *Interface Partners Int’l Ltd. v. Hananel*, 575 F.3d 97, 100, 103 (1st Cir. 2009); *Argoquest v. Israel Discount Bank, Ltd.*, 228 F. App’x 733 (9th Cir. 2007); *Henkin v. Islamic Rep. of Iran*, 2021 WL 2914036, at \*12 (D.D.C. July 12, 2021); *Fahrner-Miller Assocs., Inc. v. Mars Antennas & RF Sys., Ltd.*, 2014 WL 6871550, at \*2 (N.D. Cal. Dec. 4, 2014); *Corrie v. Caterpillar, Inc.*, 403 F. Supp. 2d 1019, 1026 (W.D. Wash. Nov. 22, 2005); *Wilson v. ImageSat Int’l N.V.*, 2008 WL 2851511, at \*6 (S.D.N.Y. July 22, 2008).

“when the defendant is ‘amenable to process’” there, *Piper Aircraft Co. v. Reyno*, 454 U.S. 235, 254 n.22 (1981), and NSO is an Israeli citizen amenable to process in Israel (Compl. ¶¶ 20-22; Shohat Decl. ¶ 5). Plaintiff also “will not be deprived of all remedies or treated unfairly” in Israel, *Tang*, 656 F.3d at 248, because “Israeli tort law provides adequate remedies for plaintiffs injured as a result of tortious conduct,” *Corrie*, 403 F. Supp. 2d at 1026. That includes claims under the Israeli Computers Law (Blecher Decl. ¶ 9) and claims for intentional infliction of emotional distress, *Henkin v. Iran*, 2021 WL 2914036, at \*12 (D.D.C. July 12, 2021). Such claims would permit remedies similar to those in the United States, including damages and injunctive relief. (Blecher Decl. ¶ 9.)

**B. The “private factors” favor dismissal.**

The “private” *forum non conveniens* factors favor dismissal. Those factors “include the ‘relative ease of access to sources of proof; availability of compulsory process for attendance of unwilling, and the cost of obtaining attendance of willing, witnesses; possibility of view of premises, if view would be appropriate to the action; and all other practical problems that make trial of a case easy, expeditious and inexpensive.’” *Tang*, 656 F.3d at 249 (cleaned up).

Here, “the most relevant private interest factors are ‘the relevant ease of access to sources of proof’ and ‘availability of compulsory process’ to obtain the attendance of witnesses.” *Id.* at 252. NSO is an Israeli corporation with its principal place of business in Israel. (Compl. ¶¶ 20-22; Shohat Decl. ¶ 4.) All of NSO’s alleged conduct took place overseas, so the most significant documents and witnesses are in Israel or other foreign countries. The testimony of current and former NSO employees in Israel will be required to address Plaintiff’s allegations about NSO’s technology and operations. Similarly, important evidence and witnesses related to Plaintiff’s alleged treatment by Saudi Arabia and the UAE would be located in those countries. The only Virginia witness is Plaintiff, and she cannot address any issues related to NSO’s conduct. That “most of the evidence and witnesses are in” other countries favors dismissal. *Tang*, 656 F.3d at 252.

That is particularly true because much foreign evidence and many foreign witnesses will not be available in Virginia. Under the [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (*Id.* at 1.) Compounding the risk [REDACTED] is the fact that Plaintiff has thus far refused to consent to a comprehensive protective order, and in any event evidence introduced at trial presumptively becomes a matter of public record. [REDACTED]

[REDACTED] will be made public.<sup>14</sup>

Moreover, Israel's DECL expressly prohibits any Israeli citizen from “[t]ransfer[ring] defense know-how through any means ... from Israel to outside of Israel, or in Israel to a person who is neither an Israeli citizen or an Israeli resident,” unless the Israeli citizen has “received a license for such activity.” (Shohat Decl. Exh. A (DECL) § 15(a).) The DECL defines “[d]efense know-how” as including any “[i]nformation that is required for the development or production of defense equipment or its use, including information referring to design, assembly, inspection, upgrade and modification, training, maintenance, operation and repair of defense equipment or its handling in any other way,” including “technical data or technical assistance.” (*Id.* § 2.) Plaintiff's allegations focus on information about NSO's Pegasus technology that constitutes defense know-how under the DECL. And any testimony about information covered by the DECL cannot lawfully be transferred “outside of Israel.” (*Id.* § 15(a)(2).) Violations of the DECL carry criminal penalties. (*Id.* §§ 32-34.) Israeli witnesses may thus be unable to answer any questions regarding NSO's technologies if those answers are at risk of being exported. (Blecher Decl. ¶¶ 11-12); *see In re Factor VIII or IX Concentrate Blood Prods. Liab. Litig.*, 2008 WL 4866431, at \*6 (N.D. Ill. June 4, 2008) (finding no “Israeli court [would] compel the appearance of an Israeli citizen for a

---

<sup>14</sup> Discovery cannot be sought from Saudi Arabia or the UAE at all, given their immunity under the FSIA. 28 U.S.C. § 1604; *see Rubin v. Islamic Rep. of Iran*, 637 F.3d 783, 795 (7th Cir. 2011) (“[I]t is widely recognized that the FSIA's immunity provisions aim to protect foreign sovereigns from the burdens of litigation, including the cost and aggravation of discovery.”).

deposition to be used in a trial to be conducted in the United States”). Without an export license, which NSO has not been able to obtain, this Court’s and the parties’ access to critical documents and witnesses in Israel will be severely curtailed, and NSO’s due process right to defend itself will be impaired. *Casco Marine Paints & Coatings, Ltd. v. M/V LEON*, 1996 WL 544232, at \*2-3 (D. Md. June 20, 1996).

Even as to witnesses whose testimony would not be barred by foreign law, this Court “lacks authority to compel the attendance of [foreign] witnesses, greatly undermining a fact-finding effort in” Virginia. *Tang*, 656 F.3d at 252; *see also Casco Marine*, 1996 WL 544232, at \*2-3 (“[T]he lack of subpoena power for witnesses located in Greece strongly favors dismissal.”). Even if foreign witnesses agreed to travel to Virginia, the cost of transporting those witnesses would be high. And “because much of the evidence will derive from [foreign] witnesses, trial in an American court will require costly translators.” *Tang*, 656 F.3d at 252. Many of NSO’s internal documents are written in Hebrew (Shohat Decl. ¶ 4), and translating these materials into English for purposes of production and testimony would be burdensome. *Tang*, 656 F.3d at 252; *see also MGA Ent. Inc. v. Deutsche Bank AG*, 2012 WL 12892902, at \*5 (C.D. Cal. Feb. 27, 2012) (concluding that “burdensome translation efforts” was a “clear fact” favoring *forum non conveniens*).

That is not the end of the “practical problems” this action will create in Virginia. *Tang*, 656 F.3d at 249. For example, any potential judgment against NSO could be more easily enforced if entered in Israel, where NSO’s assets and operations are located. A judgment of this Court would not be “automatically” enforced in Israel. Eddy Meiri, *Foreign Judgments Enforcement in Israel*, 31 Int’l L. Practicum 39 (2018). Plaintiff would bear the burden of proving, among other conditions, that the judgment “is not in contrast to public policy.” *Id.* at 41. Even then, an Israeli court would not enforce the judgment if “the losing party was not given a reasonable opportunity to present its case” or enforcing the judgment “might be detrimental to Israel’s sovereignty or security.” *Id.* Here, [REDACTED]

[REDACTED] Accordingly, Plaintiff would not be entitled to an “automatic” enforcement of any U.S. judgment—particularly one rendered in the absence of key

evidence. This factor “weighs strongly in favor of dismissal.” *Alternate Health USA Inc. v. Edalat*, 2022 WL 767573, at \*9 (C.D. Cal. Mar. 14, 2022); *cf. La Casa Real Estate & Inv., LLC v. KB Home of S.C., Inc.*, 2010 WL 2649867, at \*4 (M.D.N.C. June 30, 2010) (transferring venue to South Carolina because “any judgment in this matter would be more easily enforced in South Carolina”).

In addition, NSO’s presence on the BIS Entity List will hamper its defense in this lawsuit because U.S. individuals and entities cannot export various items to NSO. 15 C.F.R. § 744.11(a). The term “export” is defined broadly as any “transmission out of the United States … in any manner,” including the “electronic transmission of non-public data that will be received abroad.” *Id.* §§ 730.5(c), 734.13(a)(1). The list of prohibited items includes both “software” and “technology.” *Id.* §§ 772.1, 734.3(a)(1). “Technology” broadly includes any “[i]nformation necessary for the ‘development,’ ‘production,’ ‘use,’ operation, installation, maintenance, repair, overhaul, or refurbishing … of an item.” *Id.* § 772.1. There is no exception for technology created and owned by NSO itself. As a result, NSO’s U.S. litigation counsel cannot communicate with NSO regarding NSO’s own technology—the core subject matter of this litigation—or share with NSO substantial amounts of discovery that NSO needs to refute Plaintiff’s allegations. Exports could be permitted with a license, but the U.S. government has indicated that any license application will face a “presumption of denial.” *Id.* § 744, Supp. 4. In fact, King & Spalding applied for a license so that it could defend NSO in other U.S. litigation, and the license has not been granted. (Akro. Decl. ¶ 2.) Even NSO’s e-discovery vendor, Deloitte, has been unable to receive a license to provide NSO basic e-discovery software. (*Id.* ¶ 3.) In this age of electronic discovery, document review and production are all but impossible without basic e-discovery software. Accordingly, if this litigation were to proceed in Virginia, NSO’s counsel would be unable to communicate fully with its clients about the case.

In comparison to these burdens, Plaintiff’s Virginia residence “is not in and of itself sufficient to bar a district court from dismissing a case on the ground of *forum non conveniens*.” *Cheng v. Boeing Co.*, 708 F.2d 1406, 1411 (9th Cir. 1983). This is true even “where claims involving United States parties are involved,” *Riot Games, Inc. v. Shanghai Moonton Tech. Co.*,

2022 WL 17326150, at \*13 (C.D. Cal. Nov. 8, 2022), because “[t]he weight given to the plaintiff’s choice varies in proportion to the connection between the forum and the cause of action,” *GTE Wireless, Inc. v. Qualcomm, Inc.*, 71 F. Supp. 2d 517, 519 (E.D. Va. 1999). Here, Plaintiff’s claims against NSO are based on NSO’s alleged conduct in licensing its technology to the UAE, which has no connection to Virginia. *Supra* at 9-11. Virginia thus has little connection to Plaintiff’s claims, and the burden to NSO of litigating in Virginia outweighs Plaintiff’s choice of forum. See *Piper Aircraft*, 454 U.S. at 259 (“Finding that trial in the plaintiff’s chosen forum would be burdensome … is sufficient to support dismissal on grounds of *forum non conveniens*.”).

### C. The “public factors” also favor dismissal.

The “public factors” also favor dismissal, including “the administrative difficulties flowing from court congestion; the local interest in having localized controversies decided at home; … the avoidance of unnecessary problems in … the application of foreign law; and the unfairness of burdening citizens in an unrelated forum with jury duty.” *Tang*, 656 F.3d at 249 (cleaned up).

Israel “has a greater interest in this dispute” than Virginia. *Id.* at 252. Plaintiff’s claims involve the conduct of two Israeli companies that license Israeli defense technology to other governments, exclusively as allowed by the Government of Israel. (Compl. ¶¶ 20-22; Shohat Decl. ¶¶ 4-11.)

Virginia's interest, in contrast, is limited to Plaintiff's current residence in the state. But that interest is significantly reduced by the fact that Plaintiff is an Egyptian citizen who seems not to have lived in Virginia at the relevant times, and who challenges actions allegedly committed overseas by foreign governments and other foreign actors, allegedly for political reasons unrelated to Virginia. Whatever interest Virginia has in those allegations is outweighed by Israel's interest. *Cf. Cook v. Champion Tankers AS*, 2013 WL 1629136, at \*9 (N.D. Cal. Apr. 16, 2013) ("California has little interest in litigation arising out of events that took place in Asia and in which the vast majority of the individuals and property involved has no connection to the United States.").

Litigation would also needlessly burden this Court out of proportion to Virginia's limited

interest. This suit would be difficult and costly to try given the complicated technical matters at issue, the anticipated length of the trial, the sensitivity of the evidence, the likely media interest, and the complications involved in managing discovery under Israeli and U.S. legal regimes. Because of the Israeli DECL [REDACTED], the Court “would likely encounter complex issues of [Israeli] law” that Israeli courts are better equipped to resolve. *Tang*, 656 F.3d at 252. When “the local interest in [the] controversy is weak as compared to the alternative forum’s interest,” these burdens “are not justified.” *Edalat*, 2022 WL 767573, at \*11 (C.D. Cal. Mar. 14, 2022).

### **III. PLAINTIFF DOES NOT STATE A CLAIM AGAINST NSO.**

Even if this case were not barred for the reasons above, Plaintiff fails to plead a valid claim.

#### **A. Plaintiff does not state a CFAA claim.**

Plaintiff’s CFAA claim should be dismissed because she lacks statutory standing, her claim is time-barred, she does not plead any CFAA violation by NSO, and she cannot hold NSO liable for Saudi Arabia’s and the UAE’s alleged conduct.

##### **1. Plaintiff lacks statutory standing to bring a private CFAA claim.**

Plaintiff does not plead facts establishing statutory standing to bring her CFAA claim. To assert a CFAA claim, a plaintiff must have “suffere[d] damage or loss.” Plaintiff does not adequately allege she suffered any qualifying “damage” or “loss” as the CFAA defines those terms.

First, Plaintiff does not plead she suffered “damage.” The CFAA’s definition of “damage” requires “impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). That definition “[l]imit[s] ‘damage’” to “technological harms—such as the corruption of files.” *Van Buren v. United States*, 141 S. Ct. 1648, 1659-60 (2021). As a result, the majority of courts—including within the Fourth Circuit—have held that “damage” requires “alteration or erasure” of “data.” *Phreesia, Inc. v. Certify Global, Inc.*, 2022 WL 911207, at \*7-9 (D. Md. Mar. 29, 2022).<sup>15</sup> Plaintiff alleges no such “damage” caused by Saudi Arabia’s and the UAE’s

---

<sup>15</sup> See also, e.g., *Calendar Research LLC v. StubHub, Inc.*, 2020 WL 4390391, at \*22 (C.D. Cal. May 13, 2020); *NetApp, Inc. v. Nimble Storage, Inc.*, 2015 WL 400251, at \*11-15 (N.D. Cal. Jan. 29, 2015); *Pediatric Nephrology Assocs. of S. Fla. v. Variety Children’s Hosp.*, 226 F. Supp. 3d

alleged access to her devices. She does not allege any “diminution in the completeness or usability of data or information” on her devices. *Id.* at \*8 (cleaned up). She alleges only that Saudi Arabia and the UAE used NSO’s technology to access private information stored on her devices. Such “unauthorized access, copying, exporting, and misuse of data and information” is not “damage.” *Id.*

Plaintiff also does not plead “loss,” which “likewise relates to costs caused by harm to computer data, programs, systems, or information services.” *Van Buren*, 141 S. Ct. at 1659-60 (citing 18 U.S.C. § 1030(e)(11)). Consequential damages such as “the costs of fleeing to the United States” and “the loss of her and her husband’s income” (Compl. ¶ 145) do not qualify as “loss” under the CFAA unless they were “incurred because of interruption of service,” which Plaintiff does not (and cannot plausibly) allege. 18 U.S.C. 1030(e)(11); *see Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 653 (E.D. Va. 2010) (holding lost revenue was not CFAA “loss”); *CoStar Realty Info., Inc. v. Field*, 737 F. Supp. 2d 496, 513-15 (D. Md. 2010) (same). And Plaintiff’s bare assertion that she “replac[ed] her devices” (Compl. ¶ 145) is not sufficient because Plaintiff pleads no factual detail about those alleged purchases, and “payment alone is insufficient to establish that any purported [losses] were necessary or related to a CFAA violation.” *OSI Sys., Inc. v. KM-Logix, LLC*, 2022 WL 2292725, at \*3 (E.D. Va. June 24, 2022).

Even if Plaintiff’s alleged replacement devices could qualify as loss, she does not allege their cost exceeded the statutory minimum of \$5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(I). Plaintiff cannot rely on the alternate basis that the alleged “offense caused … physical injury,” *id.* § 1030(c)(4)(A)(i)(III), because she does not allege the CFAA violation *caused* injury to her or Mr. Khashoggi. Plaintiff’s only alleged physical injury resulted from “being held and interrogated by UAE officials,” which was not caused by a CFAA violation. (Compl. ¶ 147.) Plaintiff also does not allege any basis to conclude that Mr. Khashoggi’s death was caused by a CFAA violation. (Compl. ¶¶ 114-21.) Mr. Khashoggi was allegedly killed at the Saudi consulate in Istanbul (Compl. ¶ 117), to which he had traveled to receive documentation necessary to marry Ms. Cengiz. *Cengiz*,

---

1346, 1354-55 (S.D. Fla. 2016).

2022 WL 17475400, at \*2-3. Plaintiff does not allege Mr. Khashoggi traveled to or was found at the Saudi consulate due to any information gathered from Plaintiff's device.

**2. Plaintiff's CFAA claim is time-barred.**

The CFAA has a two-year statute of limitations, which runs from "the date of the act complained of or the date of the discovery of the damage." 18 U.S.C. 1030(g). When a plaintiff does not suffer "damage" as that term is defined in the CFAA, the statute of limitations runs from "the date of the act complained of." *Phreesia*, 2022 WL 911207, at \*6, 9; *State Analysis, Inc. v. Am. Fin. Servs. Ass'n*, 621 F. Supp. 2d 309, 313 (E.D. Va. 2009) (Brinkema, J.). As explained above, Plaintiff does not plead "damage" because she does not plead any "diminution in the completeness or usability of data or information" on her devices. *Phreesia*, 2022 WL 911207, at \*8 (cleaned up); *supra* at 22-23. The CFAA's statute of limitations thus began to run on "the date of the act complained of." *Id.* at \*9; *State Analysis*, 621 F. Supp. 2d at 316. The latest possible date in Plaintiff's Complaint is "July 10, 2018," more than two years before Plaintiff filed suit on June 15, 2023. (Compl. ¶ 135.) Her CFAA claim is time-barred. *State Analysis*, 621 F. Supp. 2d at 316.

**3. Plaintiff does not plead any CFAA violation by NSO.**

Plaintiff's CFAA claim depends on the alleged "access" to her devices (Compl. ¶¶ 136, 138), but her Complaint contains no factual allegation that NSO accessed her devices. She alleges only that the UAE (and maybe Saudi Arabia) accessed her devices. *Supra* at 9-11. Plaintiff thus does not plead any facts establishing a CFAA violation by NSO.

Even if Plaintiff's allegations could support a CFAA claim against Saudi Arabia or the UAE, any CFAA violation by those countries cannot be attributed to NSO. As an initial matter, "CFAA liability" cannot "be premised on 'indirect access.'" *Blades of Green, Inc. v. Go Green Lawn & Pest, LLC*, 2023 WL 5278654, at \*5 (D. Md. Aug. 16, 2023). "Allowing someone who 'directs, encourages, or induces' someone else to access a computer to be liable seems to criminalize the use of the accessed information, not the act of accessing the computer database itself." *Id.*; see *Koninklijke Philips N.V. v. Elec-Tech Int'l Co.*, 2015 WL 1289984, at \*4 (N.D. Cal.

Mar. 20, 2015) (holding that “encourag[ing]” a CFAA violation “does not support a theory of liability under the CFAA”).

The CFAA thus authorizes only one form of secondary liability: conspiracy. 18 U.S.C. § 1030(b). But Plaintiff, while making a conclusory assertion of conspiracy, does not allege any *facts* to support that assertion. To plead conspiracy, Plaintiff must allege “concrete facts” showing “an agreement” between NSO and someone to access her devices illegally. *A Soc'y Without a Name v. Virginia*, 655 F.3d 342, 346-37 (4th Cir. 2011). Specifically, she must plead “some details of the time, place and alleged effect of the conspiracy.” *Estate Constr. Co. v. Miller & Smith Holding Co.*, 14 F.3d 213, 221 (4th Cir. 1994); *see NetApp*, 2015 WL 400251, at \*8 (requiring “specific allegations of an agreement and common activities” for CFAA conspiracy). Plaintiff pleads no such facts. She does not allege any basis to conclude NSO knew—let alone agreed—that anyone, including the UAE or Saudi Arabia—would misuse Pegasus to monitor Plaintiff. Nor does she allege any details about the time or place of any agreement. Absent such factual allegations, Plaintiff’s “bare assertion of conspiracy” is inadequate. *Soc'y Without a Name*, 655 F.3d at 346.<sup>16</sup>

Plaintiff also claims NSO aided and abetted Saudi Arabia and the UAE, but the CFAA does not authorize aiding and abetting liability in civil actions. While Congress has enacted “a general aiding and abetting statute applicable to all federal crimes,” it “has not enacted a general civil aiding and abetting statute.” *Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 181-82 (1994). Whether a federal statute creates civil aiding and abetting liability thus depends on the specific statutory text. *Id.* at 182-83. And when Congress “impos[es] aiding and abetting liability,” it does so explicitly, “us[ing] the words ‘aid’ and ‘abet’ in the statutory text.” *Id.* at 177 (citing examples). Absent such an “explicit provision” providing for “aiding and

---

<sup>16</sup> *See NetApp*, 2015 WL 400251, at \*8-9 (dismissing CFAA conspiracy claim because plaintiff “plead[ed] no facts” showing defendants “agreed, cooperated, encouraged, or ratified and adopted each other’s acts”); *DTC Energy Grp. v. Hirschfeld*, 420 F. Supp. 3d 1163, 1185 (D. Colo. 2019) (holding “alleg[ation] that defendants ‘conspired’ to violate the CFAA” was “a legal conclusion couched as a factual allegation that the [c]ourt need not accept”).

abetting” liability, “courts should not implicitly read secondary liability into [a] statute.” *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1006 (9th Cir. 2006).

The CFAA contains no provision providing for civil aiding and abetting liability. The “statute’s plain language sets forth who is liable”: “a primary violator, a person who attempts a primary violation, and a co-conspirator of a primary violator.” *Flynn v. Liner Grode Stein Yankelevitz Sunshine Regenstreif & Taylor LLP*, 2011 WL 2847712, at \*3 (D. Nev. July 15, 2011); *see* 18 U.S.C. § 1030(a)-(b). That language does not encompass aiders and abettors. *Podium Corp. Inc. v. Chekkit Geolocation Servs., Inc.*, 2021 WL 5772269, at \*8-9 (D. Utah Dec. 6, 2021). To the contrary, Congress implicitly *excluded* aiding and abetting liability by imposing secondary liability only on co-conspirators. 18 U.S.C. § 1030(b). “The fact that Congress chose to impose some forms of secondary liability, but not others, indicates a deliberate congressional choice with which the courts should not interfere.” *Cent. Bank*, 511 U.S. at 184. For these reasons, this Court should join the many others that have held the CFAA does not create civil aiding and abetting liability. *E.g.*, *Podium Corp.* 2021 WL 5772269, at \*8-9; *DHI Grp. v. Kent*, 2017 WL 1088352, at \*7 (S.D. Tex. Mar. 3, 2017); *Advanced Fluid Sys. v. Huber*, 28 F. Supp. 3d 306, 328 (M.D. Pa. 2014); *Flynn*, 2011 WL 2847712, at \*3.

Even if the CFAA authorized civil aiding and abetting liability, Plaintiff does not adequately allege that NSO aided and abetted any CFAA violation. To plead aiding and abetting, Plaintiff must allege facts showing that NSO had both “knowledge of” Saudi Arabia’s and UAE’s violation and “intent to bring about that result.” *United States v. Burgos*, 94 F.3d 849, 873 (4th Cir. 1996); *see Aziz v. Alcolac, Inc.*, 658 F.3d 388, 401 (4th Cir. 2011) (holding that aiding and abetting violation of Alien Tort Statute requires “substantial assistance with the purpose of facilitating the alleged violation”). Plaintiff does not plead any facts suggesting that NSO either knew or intended that Saudi Arabia and the UAE would illegally access Plaintiff’s devices.

## **B. Plaintiff’s state law claims fail.**

### **1. Plaintiff cannot sue NSO under Virginia law.**

Plaintiff’s claims under Virginia law should be dismissed because Virginia law does not

apply to NSO’s alleged conduct. “[I]t is ordinarily presumed that state laws are intended to apply only within the state’s territorial jurisdiction and not extraterritorially.” *Westwind Acquisition Co. v. Universal Weather & Aviation, Inc.*, 668 F. Supp. 2d 749, 752 (E.D. Va. 2009). As a result, Virginia has recognized that its laws cannot be given “extraterritorial effect.” *Sherley v. Lotz*, 200 Va. 173, 176 (1958); *W. Union Telegraph Co. v. Davis*, 114 Va. 154, 156 (1912). Separately, the Due Process Clause of the U.S. Constitution prohibits Virginia from applying its law extraterritorially. *See Carolina Trucks & Equip., Inc. v. Volvo Trucks of N. Am., Inc.*, 492 F.3d 484, 489-90 (4th Cir. 2007); *Adventure Commc’ns, Inc. v. Ky. Registry of Election Fin.*, 191 F.3d 429, 435 (4th Cir. 1999); *Wynne v. I.C. Sys., Inc.*, 124 F. Supp. 3d 734, 743-44 (E.D. Va. 2015).

Plaintiff’s state law claims would involve an impermissible extraterritorial application of Virginia law because she challenges actions NSO allegedly committed overseas. As explained above, Plaintiff does not allege any facts showing that NSO accessed her devices in Virginia (or anywhere else). Any conduct NSO allegedly committed—such as designing or licensing its technology to the UAE—would have occurred in Israel or other foreign countries. Virginia law does not and cannot apply to such foreign conduct.

## 2. Plaintiff does not state a VCCA claim.

Extraterritoriality aside, Plaintiff does not plead adequate facts to state a claim under the VCCA. That is because, as with her CFAA claim, Plaintiff does not allege that NSO did anything that violates the VCCA—the only entities that allegedly accessed Plaintiffs’ devices were the UAE and maybe Saudi Arabia. *Supra* at 9-11. Plaintiff cannot sue NSO under the VCCA for those countries’ alleged actions. *First*, the VCCA does not apply to foreign governments at all. It applies only to “persons,” defined as “any individual, partnership, association, corporation or joint venture.” Va. Code § 18.2-152.2. That definition does not cover governments. *See Return Mail, Inc. v. USPS*, 139 S. Ct. 1853, 1862-63 (2019) (discussing “presumption that ‘person’ does not include” the government). *Second*, the VCCA contains no provision authorizing secondary liability. *See* Va. Code §§ 18.2-152.4, 18.2-152.12. *Third*, Plaintiff pleads no basis to hold NSO secondarily liable for Saudi Arabia’s or the UAE’s alleged actions. *Supra* at 25-26.

**3. Plaintiff does not state a claim for IIED.**

The Court should also dismiss Plaintiff's claim for intentional infliction of emotional distress ("IIED"). Such a claim is "not favored" under Virginia law, *Supervalu, Inc. v. Johnson*, 276 Va. 356, 370 (2008), and is not appropriate here.

**First**, Plaintiff does not adequately allege that NSO's alleged conduct was "outrageous or intolerable." *Id.* Conduct is not outrageous and intolerable "[e]ven if a defendant has intended to inflict emotional distress, or his conduct can be characterized by 'malice.'" *Russo v. White*, 241 Va. 23, 27 (1991) (cleaned up). "Liability has been found only where the conduct has been so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community." *Id.* (cleaned up); *see Harris v. Kreutzer*, 271 Va. 188, 204 (2006) (same). Plaintiff identifies no such outrageous conduct by NSO. The conduct she describes as outrageous—the alleged access to her devices (Compl. ¶ 184)—was allegedly committed by Saudi Arabia and UAE. NSO's only alleged conduct was licensing its technology, which is not outrageous or intolerable as required for IIED liability.

**Second**, Plaintiff does not allege sufficiently "severe" distress. *Harris*, 271 Va. at 204. Plaintiff alleges she has suffered "fear, anxiety, and extreme stress" (Compl. ¶ 184), which is no different from allegations the Virginia Supreme Court has held to be insufficient. *Harris*, 271 Va. at 204 (allegations of "severe psychological trauma and mental anguish," including "nightmares, difficulty sleeping, extreme loss of self-esteem and depression," and "mortification, humiliation, shame, disgrace, and injury to reputation"); *Russo*, 241 Va. at 28 (allegations plaintiff was "nervous, could not sleep, experienced stress ..., withdrew from activities, and was unable to concentrate at work").

**Third**, Plaintiff does not allege NSO's conduct was "directed at" her. *Supervalu*, 276 Va. at 371. A "requirement for any claim of intentional infliction of emotional distress is that the alleged harmful conduct was directed intentionally toward the affected individual." *Id.* Plaintiff does not allege that NSO specifically directed its alleged conduct of licensing its technology at her.

**4. Plaintiff does not state any negligence-based claim.**

Plaintiff's two negligence-based claims—negligence and negligent infliction of emotional distress—should both be dismissed because Plaintiff does not allege any facts that would establish that NSO owed her a duty of care. Plaintiff claims NSO owed her a duty “to not create an unreasonable risk of harm from the use of its … technology,” which NSO allegedly breached by “marketing and selling [its] spyware to countries with long histories of human rights abuses.” (Compl. ¶¶ 166, 171.) Specifically, Plaintiff alleges that NSO “did nothing to prevent [Plaintiff] from being targeted” by Saudi Arabia and the UAE. (Compl. ¶ 64.) But the Virginia Supreme Court has “consistently held that ‘generally a person does not have a duty to protect another from the conduct of third persons.’” *Burns v. Gagnon*, 283 Va. 657, 668 (2012). For such a duty to exist, a defendant must have “a special relationship” with the plaintiff. *Id.* at 668-69; *see* Peter Nash Swisher et al., Va. Prac. Tort and Personal Injury Law § 3:10. Plaintiff does not allege she had any such special relationship with NSO. Therefore, she cannot establish that NSO had a duty to protect her from any alleged conduct by Saudi Arabia or the UAE.

Plaintiff's claim for negligent infliction of emotional distress should be dismissed for the additional reason that, as with her IIED claim, she does not allege outrageous conduct by NSO or severe mental distress. *Supra* at 28. She also does not allege the distinct “*physical injury*” required for negligent infliction of emotional distress. *King v. City of Chesapeake*, 478 F. Supp. 2d 871, 873 (E.D. Va. 2007) (citing authority); *see* Va. Prac. Tort and Personal Injury Law §§ 11:4, 11:5. Plaintiff alleges only that she has suffered “emotional distress and mental suffering” (Compl. ¶ 189), not the required “*physical injury*” distinct from “an underlying emotional disturbance.” *King*, 478 F. Supp. 2d at 873-74; *accord Clagett v. Allstate Ins. Co.*, 71 Va. Cir. 105 (2006).

**5. Plaintiff does not state a claim for trespass to chattels.**

Finally, Plaintiff does not state a claim for trespass to chattels because she does not plead facts showing that NSO “intentionally use[d] or intermeddle[d] with [her] personal property.” *OSI*, 2022 WL 2292725, at \*3. As previously explained, Plaintiff alleges only that the UAE and maybe Saudi Arabia—not NSO—accessed her devices. In addition, Plaintiff does not adequately allege

her devices were “impaired as to [their] condition, quality, or value,” because “merely copying information … is insufficient to state a claim for trespass to chattels.” *Id.* (internal quotation marks omitted); *accord SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 621 (E.D. Va. 2005).

## CONCLUSION

The Court should dismiss Plaintiff’s Complaint with prejudice.

DATED: September 29, 2023

KING & SPALDING LLP

By: /s/ Edmund Power

ASHLEY C. PARRISH (Bar No. 43089)

aparrish@kslaw.com

EDMUND POWER (Bar No. 65841)

epower@kslaw.com

KING & SPALDING LLP

1700 Washington Ave., NW, Suite 900

Washington, DC 20006

Telephone: (202) 737-0500

Facsimile: (202) 626-3737

JOSEPH N. AKROTIRIANAKIS (pro hac vice)

jakro@kslaw.com

KING & SPALDING LLP

633 West Fifth Street, Suite 1700

Los Angeles, CA 90071

Telephone: (213) 443-4355

Facsimile: (213) 443-4310

*Attorneys for Defendants NSO GROUP TECHS.  
LTD. and Q CYBER TECHS. LTD.*